HEALTH IT Policy Committee

Tiger Team Recommendations on Security of ePHI

Deven McGraw
Director, Health Privacy Project
May 10, 2011

What is the “Tiger Team”?

- First assembled in June 2010 to address some specific questions from ONC that needed to be addressed by the end of the summer.
- Comprised of members of the Health IT Policy and Standards Committees, and NCVHS.
- Initial aggressive summer 2010 schedule – average of 3 phone meetings every 2 weeks, at 3-4 hours per meeting

Health IT Policy Committee Tiger Team Recommendations

- Focus has been on policies to govern exchange coming out of Stage 1 of Meaningful Use (treatment & care coordination, quality reporting, public health); mostly focused on “push” transactions
  - Limited set of health care activities/transactions
- Recommendations to ONC – what policy levers to enforce?
  - Meaningful use & certification
  - Grant conditions

Health IT Standards Committee

- Establishes standards and technical requirements for certified EHRs
- First out of the gate with security functionalities required for certified EHRs for Stage 1.
  - Encryption of data at rest and in motion
  - Access Control
  - Emergency access
  - Auto log-off after inactivity
  - Audit log
  - Integrity (use of hashing algorithm ≥ SHA-1

Matching Patients with their Information

- Use of any particular data field should not be required for matching. However, when a data field is used to match, standardized formats help increase accuracy.
  - Standards committee should recognize standard formats for commonly used data fields
  - Standards committee should develop standard for representing missing data
- Health care entities should evaluate the efficacy of their matching strategies and use such evaluations to

Matching Patients to their Information (cont.)

- Matching accuracy should be enforced through HIE/NwHIN governance
  - HIEs should implement matching accuracy programs that are appropriate for the populations served and purposes for which data is exchanged
- ONC should establish a program or programs to develop and disseminate best practices in improving data capture and matching accuracy.

Exchange Requirements for Entities

- All entities involved in electronic health information exchange should be required to have digital certificates
- Entities must demonstrate they are a legitimate business and engaged in health care transactions; credentialing organizations should rely on existing criteria/processes (like the NPI) when appropriate
- Multiple credentialing organizations will need to be recognized to meet need

Identification and authentication – Provider EHR Users

- Provider entities are responsible for identity proofing individual users
- More than single factor authentication should be required as a baseline for remote access
  - But need not be as stringent as NIST or DEA criteria
  - Certified EHRs must be tested for ability to meet DEA standard for e-prescribing controlled substances
- ONC should develop and disseminate evidence about best practices; policies should keep up with

Identification and authentication – patient users of portals to EHRs

- Entities should set their own identification requirements; Tiger Team recommended principles that include knowing your population and not setting bar so high that you discourage participation
- Single factor authentication is sufficient as baseline policy – but entities can offer greater protections (as long as bar not set so high participation is

Additional Recommendations – Patient Portals

- Entities should deploy audit trails for portals and make them available to patients upon request
- Portals should include provisions for data provenance, which is accessible to the user, both respect to access and upon download
- Portals should include mechanisms to ensure information in the portal can be securely downloaded to a third party

Security Risk Assessment for Meaningful Use Stage 2

- For Stage 2 of meaningful use, providers and entities should have to do a security risk assessment (just as in Stage 1)
- For Stage 2, providers and entities must address encryption/security functionalities for data at rest. Must attest that they have done this as part of their required security risk assessment.

Questions?

Deven McGraw

202-637-9800 x115

deven@cdt.org

www.cdt.org/healthprivacy